REMARKS

Reconsideration of this Application is respectfully requested. In response to the Office Action mailed May 2, 2005, Applicant has amended the specification. Claims 1-19 are pending.

Based on the above Amendment and the following Remarks, Applicant respectfully requests that the Examiner reconsider and withdraw all outstanding rejections.

Rejections under 35 U.S.C. §103

On pages 2-13, the Action rejects claims 1-19 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,591,249 to Zoka (hereinafter Zoka) in view of U.S. Patent No. 6,529,885 to Johnson (hereinafter Johnson).

Applicant respectfully traverses the rejection as the Action fails to establish a prima facie case of obviousness. In order to establish a prima facie case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. See M.P.E.P. § 2143.

(A) For at least the following reasons, the Action does not establish a *prima facie* case of obviousness to reject claim 1 based on the combined teachings of Zoka and Johnson.

Claim 1 recites: "A biometric authentication system comprising a first enterprise system, a second enterprise system, and a communication network interconnecting the first enterprise system and the second enterprise system, wherein: the first enterprise system includes a registration apparatus for acquiring a user's biometric information in advance of authentication, extracting features therefrom, and converting the features to **template data**, a first authentication apparatus for acquiring the user's biometric information during authentication, extracting features therefrom, and converting the features to authentication data, and a first database server apparatus for receiving the template data from the registration apparatus, storing and managing the template data, receiving the authentication data from the first authentication apparatus during authentication, comparing the authentication data with the template data, and thereby authenticating the user; and the second

enterprise system includes a second authentication apparatus for acquiring the user's biometric information, extracting features therefrom, and converting the features to authentication data, and a second database server apparatus for receiving the authentication data from the second authentication apparatus, **requesting corresponding template data** from the first database server apparatus, receiving the corresponding template data from the first database server apparatus, **comparing** the authentication data with the **corresponding template data**, thereby authenticating the user, and **storing and managing the template data** if the user is authenticated successfully." (Emphasis added).

Zoka and Johnson do not teach or suggest "a registration apparatus for acquiring a user's biometric information in advance of authentication, extracting features therefrom, and converting the features to **template data**, . . . a first database server apparatus for . . . storing and managing the template data, and "a second database server apparatus for receiving the authentication data from the second authentication apparatus, **requesting corresponding template data** from the first database server apparatus, receiving the corresponding template data from the first database server apparatus, **comparing** the authentication data with the corresponding **template data**, thereby authenticating the user, and **storing and managing the template data** if the user is authenticated successfully," (emphasis added) as recited in claim 1.

On page 3, the Action admits that:

> "Zoka does not teach a second database server apparatus for receiving the authentication data from the second authentication apparatus, requesting corresponding template data from the first server apparatus, receiving the corresponding template data from the first database server apparatus, comparing the authentication data with the corresponding template data, thereby authenticating the user, and storing and managing the received template data if the user is authenticated successfully."

Thus, by admission, the Action states that Zoka does not teach the above identified missing claim features.

On page 4, the Action alleges that Johnson teaches the above missing features in FIG. 2, col. 6, lines 31-49, and col. 12, line 27 – col. 14, line 19. The Applicant respectfully disagrees. As discussed below, Johnson only discloses a system where a Web Buyer's home bank uses a comparison of an encrypted password to authorize payment of a iDraft™ transaction presented by a Web Seller, and does not teach or suggest a system where the Web seller's site receives the

encrypted password from the Web Buyer's home bank, and further Johnson does not teach or suggest the Web Seller's site comparing an encrypted password provided by the Web buyer with the received encrypted password.

In FIG. 2, Johnson discloses a process for authorizing payment from a Web user's bank to a Web seller. A Web buyer transmits a purchase request through a Web seller's website (see Johnson, col. 12, lines 32-37). Bank iDraft™ software at the Web seller's site, which is maintained and controlled by a participating iDraft™ bank, such as the Web seller's home bank, requests and receives the Web buyer's identification information, which includes a Web buyer's ID that identifies a Web buyer's home bank, from the Web buyer's personal computer across a secure communications channel (see Johnson, col. 12, lines 43-56). The bank iDraft™ software at the Web Seller's site receives the Web buyer's identification information and executes an iDraft™ transaction (see Johnson, col. 12, lines 62-65).

Before the iDraft™ transaction is honored by the Web buyer's home bank, the Web buyer is authenticated (see Johnson, col. 12, lines 65-67). The iDraft™ software of the Web buyer's home bank requests a Web buyer's password, which is encrypted by the iDraft™ software at the Web buyer's home bank (see Johnson, col. 13, lines 5-15). The Web buyer's home bank compares the encrypted password with a previously stored and encrypted password corresponding to an ID provided by the Web buyer to authenticate the Web buyer (see Johnson, col. 13, lines 5-15, 20-24, 42-45). If the two encrypted passwords match (and correspond to the proper ID), the Web buyer is authenticated (see Johnson, col. 13, lines 42-45). Once authorized, payment is released and the Web buyer's account is debited (see Johnson, col. 13, lines 49-54). For a future transaction, the Web seller may contact the Web buyer's bank home bank automatically for authentication of a further iDraft™ transaction for the Web buyer's next purchase (see Johnson, col. 14, lines 13-19).

For at least the following three reasons, Johnson does not teach or suggest the following features the Action indicates as not being disclosed in Zoka.

First, Johnson does not teach or suggest a second database server for "**requesting corresponding template data** from the first database server apparatus, receiving the corresponding template data from the first database server apparatus," as recited in claim 1. Nowhere does Johnson teach or suggest that the Web Seller's iDraft™ software requests or receives the encrypted

password from the Web buyer's home bank iDraft™ software. In fact, only the Web buyer's home bank (to the exclusion of all other banks and the Web seller) knows and or has access to the Web buyer's encrypted password (see Johnson, col. 9, lines 55-60). Thus, Johnson does not teach or suggest a second database server for "**requesting corresponding template data** from the first database server apparatus, receiving the corresponding template data from the first database server apparatus," as recited in claim 1.

Second, Johnson does not teach or suggest a second database server for "**comparing** the authentication data with the corresponding **template data**, thereby authenticating the user," (emphasis added) as recited in claim 1. Johnson does not teach or suggest that the Web Seller's iDraft™ software compares the encrypted password received from the Web buyer with the encrypted password received from the Web Seller's home bank. Instead, only the Web Buyer's home bank is responsible for comparing the encrypted password provided by the user with a stored encrypted password (see Johnson, col. 12, lines 65-67, col. 13, lines 5-11, 20-25, 42-45). The Web Seller does not perform any such comparison. Therefore, Johnson does not teach or suggest a second database server for "**comparing** the authentication data with the corresponding **template data**, thereby authenticating the user," (emphasis added) as recited in claim 1.

Third, Johnson does not teach or suggest a second database server for "**storing and managing the template data** if the user is authenticated successfully," (emphasis added) as recited in claim 1. Johnson does not teach or suggest that the Web Seller's iDraft™ software stores and manages the encrypted password received from the Web Seller's home bank if the Web buyer is successfully authenticated. Instead, only the Web buyer's home bank stores the encrypted password (see Johnson, col. 9, lines 57-60, col. 13, lines 20-24). Consequently, Johnson does not teach or suggest a second database server for "**storing and managing the template data** if the user is authenticated successfully," (emphasis added) as recited in claim 1.

Additionally, page 4 of the Action alleges that column 6, lines 31-49 of Johnson teaches the claim features admitted as being missing from Zoka. The Applicant respectfully disagrees. This section of Johnson discloses that identification information may include a customer ID and may further include the step of storing a local master list at each of the plurality of banks, the local master list stored at each bank including the ID of each customer having presented the identification

information to that bank and the identification of the customer's home bank (see Johnson, col. 6, lines 31-37). Johnson also teaches that the master list may include a list of Web buyers identified by their ID and an identification of the Web buyers' home bank (see Johnson, col. 9, lines 63-65). However, the master list is maintained by the Web buyer's home bank to associate Web buyers by their ID with an identification of the Web buyers' home bank (see Johnson, col. 9, lines 60-65). Johnson does not teach or suggest that other banks may request the local master list from the Web Buyer's bank and also does not teach or suggest using the master list as authentication data for comparison with an encrypted password provided by the Web buyer's bank to thereby authenticate the Web buyer. Thus, Johnson does not teach or suggest a second database server for "**requesting corresponding template data** from the first database server apparatus" and "**comparing** the authentication data with the corresponding **template data**, thereby authenticating the user," (emphasis added) as recited in claim 1.

Hence, Johnson does not teach or suggest the features the Action admits that Zoka does not disclose (see Action, page 3). Thus, the Action does not establish a *prima facie* case of obviousness for combining Zoka with Johnson as the combined teachings do not teach or suggest all of the features of claim 1. Therefore, claim 1 is allowable over the cited references and allowance thereof is respectfully requested.

Claims 2-6 and 16, which depend from claim 1, are also in condition for allowance because of their dependence on an allowable claim.

(B) Claim 7 is allowable for reasons analogous to those given for claim 1. Specifically, Johnson does not teach or suggest that the Web Seller site sends "the authentication data received from the simplified registration apparatus to the" Web buyer's home bank, receives "the corresponding template data from the" Web buyer's home bank, stores and manages "the received template data," or compares "the authentication data received from the second authentication apparatus with the stored template data, thereby authenticating the user." Therefore, Johnson does not teach or suggest "a second database server apparatus for receiving the authentication data from the simplified registration apparatus and the second authentication apparatus, sending the authentication data received from the simplified registration apparatus to the first database server

apparatus, receiving the corresponding template data from the first database server apparatus, storing and managing the received template data, and comparing the authentication data received from the second authentication apparatus with the stored template data, thereby authenticating the user," as recited in claim 7.

Claim 17, which depends from claim 7, is also in condition for allowance because of its dependence on an allowable claim.

(C) For at least the following reasons, the Action does not establish a *prima facie* case of obviousness to reject claim 8 based on the combined teachings of Zoka and Johnson.

Claim 8 recites: "A database server apparatus for use in a first enterprise system that is linked by a communication network to a second enterprise system, for receiving biometric template data and biometric authentication data from the first enterprise system, storing and managing the biometric template data, comparing the biometric authentication data with the biometric template data, thereby authenticating users of the first enterprise system, and supplying the biometric template data on request to the second enterprise system to enable users of the first enterprise system to become registered with the second enterprise system." (Emphasis added).

Zoka and Johnson do not teach or suggest "supplying the biometric template data on request to the second enterprise system to enable users of the first enterprise system to become registered with the second enterprise system," as recited in claim 8. On page 9, the Action admits that Zoka "does not teach supplying the biometric template data on request to the second enterprise system to enable users of the first enterprise system to become registered wit the second enterprise system." The Action then alleges that Johnson teaches "supplying the biometric template data on request to the second enterprise system to enable users of the first enterprise system to become registered with the second enterprise system," and cites FIG. 2, col. 6, lines 31-49, and col. 12, line 27 – col. 14, line 19 of Johnson.

However, as discussed above in the remarks on claim 1, Johnson discloses providing an encrypted password to a Web Buyer's home bank for authorizing payment to a Web seller's site (see Johnson, col. 12, lines 5-24, 42-54), and does not teach or suggest supplying the encrypted password on request from the Web buyer's home bank to the Web seller's site to enable Web buyers

to become registered with the **Web seller's site**. Although Johnson teaches that the Web buyer logs onto the Web seller's site, logging onto the Web seller's site is not analogous to the claimed enabling "users of the first enterprise system to become registered with the second enterprise system" since the Web buyer's home bank does not provide the encrypted password to the Web seller's site to register the Web buyer with the Web seller's site. Hence, Johnson does not teach or suggest the claimed features of a database server apparatus for "supplying the biometric template data on request to the second enterprise system to enable users of the first enterprise system to become registered with the second enterprise system" as alleged in the Action. Thus, the Action does not establish a *prima facie* case of obviousness for combining Zoka with Johnson as the combined teachings do not teach or suggest all of the claim features of claim 8. Therefore, claim 8 is allowable over the cited references and allowance thereof is respectfully requested.

Claims 9-12 and 18, which depend from claim 8, are also in condition for allowance because of their dependence on an allowable claim.

(D) Claim 13 is allowable for reasons analogous to those given for claim 8.

Claims 14, 15, and 19, which depend from claim 13, are also in condition for allowance because of their dependence on an allowable claim.

Accordingly, claims 1-19 are in condition for allowance and allowance thereof is respectfully requested.

Conclusion

All of the stated grounds of objection and rejection have been properly traversed, accommodated, or rendered moot. Applicant therefore respectfully requests that the Examiner reconsider and withdrawn all presently outstanding objections and rejections. Applicant believes that a full and complete reply has been made to the outstanding Office Action and, as such, the present application is in condition for allowance. If the Examiner believes, for any reason, that personal communication will expedite prosecution of this application, the Examiner is hereby invited to telephone the undersigned at the number provided.

Respectfully submitted,

Dated: August 1, 2005

By _____

Michael A. Sartori, Ph.D.
Registration No.: 41,289
VENABLE LLP
P.O. Box 34385
Washington, DC 20043-9998
(202) 344-4000
(202) 344-8300 (Fax)
Attorney For Applicant